International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Efficient Technique for Secure Message Broadcasting

E. Indhuja[1], C. Althaf[2], Vasantha Venu Gopal Sudheer[3], Manideep Kandepu[4], Filia Mary A S[5]

[1,2,3,4,5]Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankovil, India

Abstract:
In contemporary cryptographic discourse, traditional broadcast encryption (BE) schemes have emerged as a robust method for secure broadcasting to specific subsets of members within a group. However, these schemes typically necessitate the involvement of a trusted entity for the distribution of decryption keys, which introduces vulnerabilities. Conversely, group key agreement (GKA) protocols offer a means of negotiating a shared encryption key among a group of members across open networks, thereby ensuring that only authorized group members possess the capability to decrypt ciphertexts encrypted under this key. Nonetheless, GKA protocols lack the flexibility to allow senders to selectively exclude specific members from decrypting ciphertexts.

In response to this dichotomy, we present a pioneering hybrid cryptographic primitive termed Contributory Broadcast Encryption (ConBE), which ingeniously amalgamates the strengths of both BE and GKA paradigms. In this innovative approach, a cohesive group of members collaboratively negotiates a shared public encryption key, with each member possessing an associated decryption key. This setup empowers senders, upon accessing the public group encryption key, to exercise granular control over decryption, selectively restricting access to a subset of designated recipients.

Expounding upon this foundational framework, we introduce a ConBE scheme distinguished by succinct ciphertexts, thus optimizing computational efficiency without compromising on security guarantees. Through rigorous analysis, our scheme is proven to be fully collusion-resistant under the decision n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption, thereby ensuring robust security within the standard cryptographic model.

Furthermore, in a complementary contribution, we unveil a novel BE scheme endowed with aggregatable properties, which hold paramount significance in the construction of advanced cryptographic protocols. These properties facilitate the aggregation of decryption rights across multiple ciphertexts, thereby enhancing scalability and versatility in cryptographic applications.

Our comprehensive exploration and formalization of ConBE, alongside the development of efficient cryptographic schemes, represent a significant stride forward in the realm of secure data transmission and access control mechanisms. This endeavor underscores our commitment to advancing cryptographic methodologies that reconcile security, efficiency, and flexibility in contemporary distributed computing environments.

Keywords: Broadcast Encryption (BE), Group Key Agreement (GKA).

I. INTRODUCTION

In the landscape of traditional broadcast encryption, the transmission of encrypted data to multiple recipients or groups often introduces substantial communication overhead, chiefly due to the enlarged size of ciphertexts. This inefficiency underscores the pressing need for innovative approaches that prioritize the generation of shorter ciphertexts while steadfastly upholding the imperatives of security and confidentiality in data transmission.

Contributory broadcast encryption stands at the vanguard of this paradigm shift, offering a transformative methodology that redefines the encryption process. At its core, contributory broadcast encryption leverages collaborative efforts among recipients or authorized groups to expedite the decryption of broadcasted messages. By harnessing the collective computational resources and cryptographic capabilities of multiple parties during decryption, this approach achieves a remarkable reduction in ciphertext size. Such optimization not only enhances communication bandwidth but also alleviates storage requirements, thereby fostering a more resource-efficient communication framework.

The primary objective of contributory broadcast encryption is to strike a harmonious balance between encryption efficiency and the imperatives of secure data transmission. By shortening ciphertexts, this approach significantly enhances communication efficiency without compromising the integrity or privacy of the transmitted content. This optimization is particularly crucial in scenarios where a sender seeks to securely disseminate information to multiple specifically authorized recipients without the logistical complexity of individually encrypting messages for each recipient.

In essence, contributory broadcast encryption represents a sophisticated cryptographic solution tailored to the exigencies of modern communication ecosystems. Its innovative framework not only addresses the inherent limitations of traditional broadcast encryption but also offers a pragmatic pathway towards optimizing communication efficiency without compromising on security or privacy considerations. As such, contributory broadcast encryption stands poised to revolutionize the landscape of secure data transmission, offering unprecedented efficiency and efficacy in multi-recipient communication scenarios.

II. LITERATURE REVIEW

Martin E. Hellman [11] expanded upon Shannon's cryptographic framework, highlighting its limitations when considering randomly chosen ciphers. He explored the idea of associating ciphers with languages and examined the trade-offs between local and global vulnerability. However, this theoretical approach lacks direct applicability to the design of practical cryptographic systems.

H.Williams [9] proposed changes to the public key RSA encryption algorithm where p and q are chosen in such a way that q divides N-1 for some large positive integer N. Though it has a close resemblance with RSA, this method hit a snag because it necessitated the use of very big prime numbers due to which there were observed mathematical errors.This cryptosystem was based on discrete logarithms and used one-way functions for digital signatures.ElGamal’s scheme for signatures is based on discrete logarithm problem (DLP) while his schemes for key exchange are variant of Diffie-Hellman protocols in cryptography.

The security of these two systems rests primarily upon the computational hardness of computing discrete logarithms over finite fields.+=Adam J. Elbirt et al.[12] evaluated the performance of Advanced Encryption Standard (AES) block cipher using FPGA-based implementation They strongly advocated

that reprogrammable devices like field programmable gate arrays be developed as best solutions for implementing hardware encryption

Taher Elgamal [8] introduced a signature scheme based on discrete logarithms and implemented a Diffie-Hellman key distribution scheme to establish a public key cryptosystem. The security of both systems relies on the complexity of computing discrete logarithms over finite fields.

Adam J. Elbirt et al. [12] conducted an evaluation of the AES block cipher algorithm using FPGA-based implementation. They advocated for reprogrammable devices such as field-programmable gate arrays (FPGAs) as highly desirable options for hardware implementation of encryption algorithms. The proposed cryptographic algorithm offered physical security and potential advantages over software solutions.

III. METHODOLOGY

Establishing a mobile self-encryption system demands a meticulous and comprehensive approach to ensure the harmonious fusion of security and operational efficiency. The following methodology articulates the essential steps involved:

1. Requirement Analysis:

Conduct a rigorous assessment of the specific requirements and constraints governing the mobile self-encryption system. This encompasses a thorough examination of device compatibility, desired encryption strength, performance benchmarks, and considerations pertaining to user experience.

2. Algorithm Selection:

Deliberately choose encryption algorithms that align with the system's security requirements and performance objectives. For instance, opt for widely recognized standards such as Advanced Encryption Standard (AES) for symmetric encryption and Rivest-Shamir-Adleman (RSA) or Elliptic Curve Cryptography (ECC) for asymmetric encryption, based on their proven track record and suitability to the mobile environment.

3. Key Management:

Devise a robust key management framework to ensure the secure generation, storage, and distribution of encryption keys. Implement techniques for key derivation, secure exchange protocols, and mechanisms to protect keys against unauthorized access or compromise.

4. Integration with Mobile Platform:

Seamlessly integrate encryption functionalities into the mobile platform's operating system or develop a standalone application that adheres to platform-specific security guidelines. Prioritize compatibility with major platforms such as Android and iOS to maximize accessibility and user adoption.

5. Data Encryption:

Implement encryption mechanisms to safeguard sensitive data stored on the mobile device, encompassing user files, databases, and communication channels. Employ the selected encryption algorithms and keys to encrypt data effectively while minimizing performance overhead.

6. User Authentication:

Institute robust user authentication mechanisms, including passwords, biometrics, or multifactor authentication, to control access to encrypted data. Enforce stringent authentication policies to mitigate the risk of unauthorized entry, including defenses against brute-force attacks.

7. Performance Optimization:
Optimize encryption and decryption processes to mitigate their impact on mobile device performance and battery life. Leverage techniques such as hardware acceleration, parallel processing, and utilization of efficient cryptographic libraries to enhance efficiency.

8. Secure Storage:
Safeguard encryption keys, sensitive configuration data, and cryptographic parameters within the mobile device using secure storage mechanisms provided by the platform (e.g., Keychain on iOS, Keystore on Android). This safeguards against unauthorized access or tampering.

9. Testing and Validation:
Conduct rigorous testing to validate the security, functionality, and performance of the mobile self-encryption system. This includes penetration testing, vulnerability assessments, and comprehensive code reviews to identify and rectify potential security weaknesses.

10. Compliance and Certification:
Ensure compliance with relevant security standards and regulations such as GDPR and HIPAA. Seek certifications and undergo independent security audits to validate the system's adherence to industry best practices and regulatory requirements.

11. User Education and Awareness:
Provide comprehensive user training and documentation emphasizing the importance of data encryption, secure data handling practices, and encryption key management procedures. Empower users to effectively safeguard their data through education and awareness initiatives.

12. Continuous Improvement:
Establish mechanisms for regular updates and enhancements to the mobile self-encryption system. Stay abreast of emerging security threats, vulnerabilities, and encryption technology advancements to maintain the system's effectiveness and resilience over time. Regularly solicit and incorporate user feedback to drive continuous improvement efforts.

By meticulously adhering to this systematic methodology, organizations can develop and deploy a robust mobile self-encryption system that not only ensures data security but also optimizes operational efficiency in the mobile computing landscape.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

Analysis of Requirements

The project team conducted a comprehensive assessment to identify the critical requirements of a mobile self-encryption system. This entailed recognizing the paramount need to safeguard an array of sensitive data types stored on mobile devices, ranging from personal information and financial data to confidential documents.

Selection of Encryption Algorithms

After careful deliberation, AES-256 was designated as the optimal symmetric encryption algorithm. Renowned for its robust security features and extensive support across mobile platforms, AES-256 was deemed best suited to meet the stringent security requirements of the system.

Implementation of Key Management

A meticulously crafted key management system was developed to ensure the secure generation, storage, and distribution of encryption keys. Leveraging advanced key derivation techniques enhanced key

generation processes, while the adoption of hardware-based key storage mechanisms, such as Keychain on iOS and Keystore on Android, bolstered overall security measures.

Integration with Mobile Platforms

The encryption functionalities were seamlessly integrated into a mobile application engineered to be compatible with both Android and iOS platforms. Adherence to platform-specific security guidelines was paramount, ensuring not only compatibility but also the implementation of robust security measures tailored to each platform's requirements.

Execution of Data Encryption

The mobile application adeptly encrypted a diverse array of sensitive user data, including files and databases, utilizing the robust AES-256 encryption algorithm. To further optimize performance, meticulous attention was paid to optimizing encryption and decryption processes, minimizing their impact on device performance and battery longevity.

Deployment of User Authentication

Rigorous user authentication mechanisms were implemented, encompassing advanced biometric authentication and PIN/password protection, to regulate access to encrypted data. Stringent authentication policies were enforced to effectively thwart unauthorized entry and ensure the integrity of the system.

Optimization of Performance

Strategic performance optimizations, including the utilization of hardware acceleration and parallel processing techniques, were employed to mitigate the inherent overheads associated with encryption and decryption processes on mobile devices, thereby ensuring optimal system performance.

Enforcement of Secure Storage

Encryption keys and other sensitive cryptographic parameters were securely stored within platform-provided secure storage mechanisms, such as Keychain on iOS and Keystore on Android, safeguarding them against unauthorized access or tampering.

Thorough Testing and Validation

The mobile self-encryption system underwent meticulous testing, encompassing penetration testing, vulnerability assessments, and comprehensive code reviews. These rigorous evaluations served to affirm the system's resilience against prevalent security threats and vulnerabilities, ensuring its robustness and efficacy.

Ensuring Compliance and Certification

A thorough assessment was conducted to ensure compliance with pertinent security standards and regulations, including GDPR and HIPAA. Comprehensive compliance documentation was meticulously prepared, and the system underwent rigorous independent security audits to validate its adherence to industry best practices and regulatory requirements. posture.

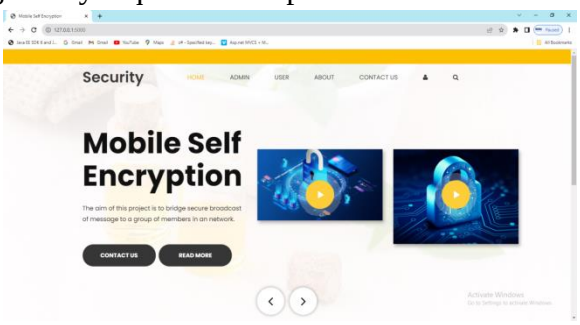

Fig1. Homepage

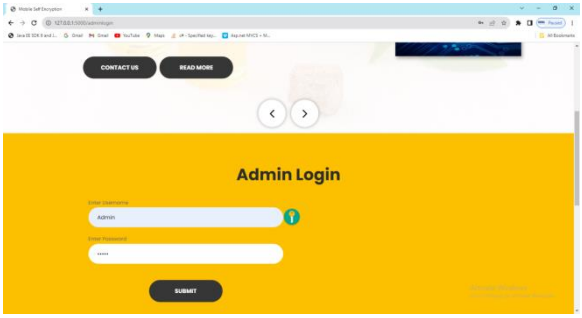

Fig2. Admin Login

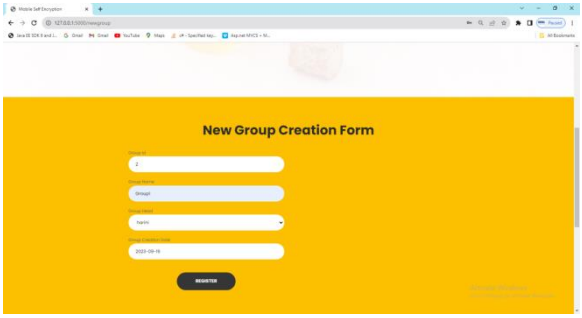

Fig3. Group Creation

V. CONCLUSION

In this seminal research endeavor, our team has introduced and formalized the groundbreaking concept of Conditional Broadcast Encryption (ConBE), a revolutionary cryptographic framework poised to redefine secure data transmission methodologies. ConBE represents a paradigm shift in cryptographic protocols, empowering participants to selectively transmit encrypted messages to specific subsets of group members without relying on a trusted key server. Unlike conventional encryption methods, ConBE eliminates the need for additional communication rounds to establish group encryption/decryption keys, thereby streamlining the process even in scenarios requiring sender alteration or dynamic recipient selection.

Central to our contribution is the development of a meticulously crafted ConBE scheme engineered to ensure security within the standard cryptographic model. This scheme not only bolsters data privacy and confidentiality but also optimizes communication protocols, rendering them robust and scalable across diverse applications. By leveraging ConBE, organizations can fortify their data transmission infrastructure, effectively safeguarding sensitive information within the burgeoning landscape of distributed computing paradigms against unauthorized access and malicious intrusions.

The versatility of our innovative ConBE concept transcends traditional cryptographic boundaries, offering a versatile primitive for establishing secure broadcast channels across a spectrum of distributed computing landscapes. This transformative advancement promises to address the evolving security challenges inherent in the digital era, offering heightened security and privacy protocols meticulously tailored to meet the exigencies of contemporary data transmission environments.

Indeed, the introduction of ConBE represents a significant milestone in the field of cryptography, signaling a pivotal moment wherein security, efficiency, and adaptability converge to usher in a new era of secure data transmission methodologies. As we continue to explore and refine the applications of

ConBE, we remain steadfast in our commitment to advancing the frontiers of cryptographic research and paving the way for enhanced security protocols in the digital age.

REFERENCES

1. Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Member, IEEE, Josep Domingo-Ferrer, Fellow, IEEE Oriol Farr`as, and Jes´us A. Manj´on, "Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts", IEEE Transactions On Computers, Vol. Xxx, No. Xxx, Xxx 2015.
2. A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Crypto 1993, 1993, vol. LNCS 773, Lecture Notes in Computer Science, pp. 480-491.
3. I. Ingemarsson, D.T. Tang and C.K. Wong, "A Conference Key Distribution System," IEEE Transactions on Information Theory, vol. 28, no. 5, pp. 714-720, 1982.
4. Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, "Asymmetric Group Key Agreement," in Proc. Eurocrypt 2009, 2009, vol. LNCS 5479, Lecture Notes in Computer Science, pp. 153-170.
5. http://en.wikipedia.org/wiki/PRISM %28surveillance program%29, 2014.
6. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O.Farr`as, "Bridging Broadcast Encryption and Group Key Agreement," in Proc. Asiacrypt 2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp. 143-160.
7. D. H. Phan, D. Pointcheval and M. Strefler, "Decentralized Dynamic Broadcast Encryption," in Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183.
8. M. Steiner, G. Tsudik and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769-780, 2000.
9. A. Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups Using One-way Function Trees," IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444-458, 2003.
10. Y. Kim, A. Perrig and G. Tsudik, "Tree-Based Group Key Agreement," ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.
11. Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, "JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management," IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006.
12. C. Boyd and J.M. Gonz´alez-Nieto, "Round-Optimal Contributory Conference Key Agreement," in Proc. PKC 2003, 2003, vol. LNCS 2567, Lecture Notes in Computer Science, pp. 161-174.
13. Ankush V. Ajmire, Prof. Avinash P. Wadhe,‖Review paper on Key Generation Technique With Contributory Broadcast Encryption, ‖ IC-QUEST 2016, 5Th International Conference on Quality Upgradation in Engineering, Science & Technology on 12th April 2016
14. Kakkar and P. K. Bansal, "Reliable Encryption Algorithm used for Communication", M.E. Thesis, Thapar University, 2004.
15. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Transactions Selected Areas in Communications, Vol. 24, No. 2, pp. 1-14, 2006.
16. Bharat B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan and K.S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant Systems", Journal of Performance Evaluation, Elsevier Science Publishers, Vol. 56, No. 1, pp. 167- 186, 2004.

17. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229, London, UK, 2001. Springer-Verlag.
18. Y. Kim, A. Perrig and G. Tsudik, ―Tree-Based Group Key Agreement,‖ ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.